المدير التنفيذي للرقابة المصرفية
Executive Director - Banking Supervision

مصرف البحرين المركزي
Central Bank of Bahrain

EDBS/KH/C/27/2016
1st June 2016

Chief Executive Officer
All Bank Licensees, Financing Cos., Card Processing and Payment Service Providers, and Credit Information Bureaus
Manama
Kingdom of Bahrain

Dear Sir,

Cyber Security Risk Management

I am writing to draw your attention to the growing importance of proper cyber-security risk management and to provide some general guidance on the matter. For the purpose of this circular cyber-attacks refer to attacks that target an institution's IT systems and networks with an aim to illegally transfer funds, disrupt, disable, destroy or maliciously control an IT system/network to destroy the integrity of the institution's data, or to steal information from it. Recent trends indicate that the frequency, stealth, sophistication and the potential impact of cyber-attacks are on the rise globally.

The CBB is currently studying the matter for the purpose of developing detailed IT Security requirements. However, in the interim, the CBB requires all Licensees to comply with the following requirements before the end of the year:

1. **Risk Ownership and management accountability** – Clear ownership and management accountability of the risks associated with cyber-attacks and related risk management measures should be established, which should cover not only the IT function but also all relevant business lines. As such an effective cyber-security risk management must be made part of the Licensees' IT security policy and procedures.

2. **Periodic evaluations and monitoring of cyber-security controls** – As the threats of cyber-attacks are evolving in nature, the Board and/or senior management should ensure that the cyber-security controls are periodically evaluated for adequacy, having regard to emerging cyber-threats and a credible benchmark of cyber-security controls endorsed by the Board and/or senior management. If material gaps are identified, the Board and/or senior management must properly address such gaps immediately.

2/...

3. **Reporting of any cyber-attack –** All instances of cyber-attacks, whether internal or external, that cause customer information to be compromised or disruption of critical services that affects the core capabilities of the Licensee should be immediately reported to the CBB within one week. The Licensee should also provide the root cause analysis of the cyber-attack and measures taken by the Licensee to avoid similar incidents in future.

4. **Business continuity –** To prepare for the eventuality of cyber-attacks, the Licensee should have a cyber-attack response mechanism in place. The Business Continuity Plan of the Licensee should also be properly enhanced to account for all CBB mandates and should be regularly tested to assure that the Licensee is capable of dealing with cyber-attacks.

If the above mentioned areas are not in place already, the Licensee should provide quarterly progress reports on the steps and procedures taken in implementing them. The progress report must be provided to the Mr. Rashed Al Muawada (17547257) via email infosecurity@cbb.gov.bh and the first report must be submitted by June 30th 2016.

Yours sincerely

Khalid Hamad